United States District Court
Northern District of California

Opperman, et al
v.
Path, Inc., et al

No: 13-CV-453-JST

Motion to Intervene as Plaintiff (Fed. Gv. P. 24)

Motion to Intervene

Relief Sought

Intervenor seeks intervention of right, and also, permissive intervention:

Justin Credico, moves this court for an Order permitting him to intervene as a plaintiff in this action as a matter of right under Rule 24 of the Federal Rules of Civil Procedure, or, in the alternative, allowing him permissive intervention as a plaintiff in this matter under Rule 24.

Claims to Be Asserted

By intervening in this action, Justin Credico, seeks to assert the enclosed claims set out in the attached Grounds for Granting Motion for Intervention, and also, seeks to obtain discovery materials related to this captioned case of Opperman et al v. Path Inc. et al (13-CV-453-JST).

Grounds for Intervention

Intervention as of right:

Justin Credico, is entitled to intervene in this action as a matter of right because;

1) He has information and experience with Apple iOS programming;
2) He also has come across the Apple Inc, et al defendants' user license agreements; and other representations to iDevices;
3) He has qualifying interest in the subject of the action;
4) He has a legally protected interest in his idevice as well as the plaintiffs, and has security information details that pertain to Apple et al defendants' statements concerning privacy and data security

5) Plaintiffs' interests in this action may be assisted, as none have explained to the court that any persons of the "idevice" class have any iOS programming experience of their own, which intervenor thinks would change pleadings in order to survive summary dismissals.

6) Intervenor has written apps for his idevice using Objective-C, an unapproved public-facing method to create Apps, nor supported by Apple.

Permissive Intervention

In the alternative, if Justin Credico's Motion for Intervention as of right is denied, intervenor should be allowed as a permissive intervenor in this action because:

1) A court may permit intervention as of right by applicant who has "a claim or defense that shares with the main action a common question of law or fact" (see Fed. R. Civ. P. 24(b)(1)(B) quoted in Ramirez v. ManPower Inc 2014 US Dist Lexis 94362 (9th Cir))

2. Intervenor satisfies this need because he, has used Apple's App Store along with Itunes Apple App Store, OSX SDK for iPhone iOS under VMware with the 32-bit Snow Leopard OSX, and also, has reviewed the Apple ULA's disclosures, UCL, FAL, CLRA.

3. He shares common questions of law pertaining to the above misrepresentations of the defendants, as to their App Store, and Apps.

4. Court interest will be best served to allow this intervention due to the knowledge of iOS programming that he has performed on his idevice.

5. Also, because of the security knowledge he has of idevices; from being a hacker, malware coder, and programmer.

Record on Motion

This matter is based upon; this motion, all Opperman v. Path Lexis Nexis records (65100, 14832, 3401, 8885, 67225) and whatever evidence and arguments which may be allowed at the hearing on this motion

Patent Prosecution Bar
"the proposed bar"

Intervenor feels as though the information contained herein, concerning iOS software and hardware, will not effect the Court's Order of the proposed bar, nor the defendants proposed bar request. Intervener will not disclose any debugging, decoding of hardware or software information, or idevice app unpacking information within this Motion. However, security and privacy flaws within the idevice design may be referenced as part of court record within this Motion.

Grounds for Intervention

Upon review of the Lexis Nexis record concerning the Opperman Lexis 67225 Order, the intervenor noticed several aspects of the information contained therein, and now divulges some information as to "iDevices" which will help the plaintiffs; the difficulties in understanding iPhone App programming and development, and the programs used upon the idevice. Information including, but not limited to, boot process, the iPhone Operating System, various ways to program or code apps, and, security and privacy issues related to these informations.

In its order, the court mentions, "Defendant Apple Inc. designs and manufactures the iPhone, the iPod Touch, and the iPad, ("iDevices") each of which is a mobile device that can wirelessly access the internet. Since 2008, those devices have included an App Store, which enables

Users to download software, or apps, to their devices created by 3rd parties. Each Defendant except Apple is an app developer (collectively, "App Defendants"). Plaintiffs allege the App defendants' apps have been surreptitiously stealing and disseminating the contact information stored by customers on Apple Devices." Intervenor, brings this Motion on behalf of those Plaintiffs of an "iDevice Class," composed of all purchasers of Apple's iDevices between July 10th 2008 and the present who downloaded the App Defendants' apps, and on behalf of 3 subclasses: "Malware," "Address Book," and "Texas Subclasses." (See CAC paragraph 48 referenced in this Court's Order)

In this case's Lexis 67225 order, the Court stated, "in sum, Apple has attempted to cultivate a perception that its products are safe and that Apple strives to protect its users" (See CAC paragraph 99)

The Court then references these representations by Apple Inc, and, its these plaintiffs' misrepresentation and disclosure counts that intervenor is concerned with. "All apps run in a safe environment, so a website or app can't access data from other apps." (see CAC paragraph 102) and, "Applications on the device are 'sandboxed' so they cannot access data stored by other applications" (see CAC paragraph 209). Lastly, the Court addressed Apple's "customer privacy policy" as Apple states it: "Apple takes precautions -including administrative, technical, and physical measures to safeguard your personal information against loss, theft, and misuse, as well as unauthorized access, disclosure, alteration, and destruction." (CAC paragraph 209)

Throughout this motion, intervenor will relate back to the portions of that customer privacy statement; unauthorized access, disclosure, alteration, and destruction. And, intervenor will explain several things concerning those, that neither Apple and defendants, nor, plaintiffs detailed before your Court

Iphones

The lovely idevice that the people have become so accustomed to seeing and using is basically a computer. The device uses the ARM processor architecture, based upon the OSx Darwin Linux OS with iOS running and serving as the GUI front end.

Iphone Apps can be programmed and made in two ways:

1) using the Apple downloadable SDK and tools that require OSX or a VMWare running an OSx image; or,

2) using Objective-C coding and compiling (this method is what the intervenor uses, and creates apps for his iPhone, while on the iPhone. (this method is entirely the most complicated as the programmer MUST write the code by hand without the SDK clickable objects - and the programmer must understand how to command line compile these apps using Non-Apple approved methods and jailbreaking -)

Now once an app is created, whether using the SDK or other command-line method (on the phone for the phone "idevice") which require the objective-c libraries, the app still CAN NOT be

installed and ran on the iDevice; the app will open and then just close out. And this is where jailbroken phones differ from a "normal phone" insofar as, installing apps. ALL APPS MUST BE CODE-SIGNED. For jailbreak phones, a program fake-sign can be used to code sign the app with a fake certificate. Whereas, in a normal phone, Apple INC allows the developer one of two types of certificates for signing apps:

1) Developer Certifications - which are good for about one-years work, costing roughly $99

2) Enterprise Certifications - mainly given and sold to major businesses that design and promote apps for Apple iDevices.

This is what allows your device to prevent apps from being installed, Apple's way of preventing malicious software installations without user's consent. If any unscrupulous developer were to get his hands on some certificate and used it to sign an app, not only will the app appear to be made by whomever this certificate is licensed to, but, so long as the app is written for the right iOS version, this app will install and run on the device with no problems.

And Apple does remain silent about how apps can easily be installed via drive-by downloading off of websites (heading to a website, that is properly coded to deliver or upload the app to your iDevice) and the intervenor believes that a Google search of: "Iphone app air [redacted] install" should put this into perspective.

Iphone App "Malware"

As it seems to your intervenor, the subclass of "malware" was given as a descriptor because of the fact that some of these apps were grabbing plaintiffs' address book contents and/or other sensitive information from the cell phone, or idevice. Your intervenor is not going to dive into the discussion of the how-to's of iphone app malware programming; as we have seen jailbreak worms such as ikeeb, the ABC News press release about new iphone malware (2014 Veterans Day) that was being installed into people's phones, and the Chinese protester Spy-App that was found circulating in the wild.

The iphone (API) application programming interface is a complicated subject, but, its these API that Apps use in order to access the idevices objects. These API are listed in the Apps code headers, when Apps are compiled, and if the developer adds any code API to an App, he or she can grab any "global data" such as; images, recordings, videos, contacts. These API can be used to do this, with or without the user's knowledge, even storing data to the phone/device (such as recording apps). Now, the "sandbox" security feature is what Apple uses to deter Apps from accessing other Apps, yet we see in this claim that even Apple suggests to take the global data if the developer so chooses.

In this case, these defendants should be able to show the Court, intervenor, and plaintiffs, all API that their apps use during compilation. This will allow the plaintiffs' to see whether or not some apps are intentionally data grabbing when there is no need to do so.

Misrepresentations

Intervenor will now tie the claims which consist of invasion of privacy and the collective "misrepresentation" claims (UCL, FAL, CLRA and intrusion/seclusion), to assist the plaintiffs in reopening or amending certain claims, and injuries.

In order to meet an intrusion upon seclusion privacy claim, the plaintiffs are required to show

1) intrusion into a private place, conversation, or matter
2) in a manner highly offensive to a reasonable person

This tort is proven only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source.

Such as: Address Books, contacts, pictures, videos, audio files, et. al. data downloaded into a persons idevice (this Court relied upon the case of Zavala)

In determining the claims under (disclosure failure, UCL, FAL, and CLRA) representations, the allegations must include "an account of time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentations" (see Opperman quoting Swartz v. KPMG LLP, 476 F.3d 756 (9th Cir.))

"Plaintiffs alleged that they saw and relied upon Apple's website, in store advertisements, and television advertising in purchasing their iDevices, and that they would have paid less for their devices, or not purchased them at all, had they known they were vulnerable to privacy attacks (see CAC paragraph 125-126) and; "Apple claims to review every app on the App store based on a set of technical, content, and design criteria and also, Section 533 Restatement Second of Torts shows that, One who makes a misrepresentation ... or conceals a material fact... "

The Court concluded that plaintiffs failed to show that they "lost money or property," and, relied upon Kwikset Corp. v. Super Ct, 51 Cal. 4th 310, 325, 120 Cal. Rptr. 3d 741, 246 P.3d 877)

The intervenor points the court to the lost property consisting of DATA in the iDevice Contacts and/or Address Books (or others that may be discoverable after intervenor assists the plaintiffs with using a packet sniffer). And, the court was to quick to dismiss the public disclosure claim due to the plaintiffs' lack of showing injury because, "they did not allege that any interception [did so] occur" (see Court's Order)

The problem with this requirement of showing that the alleged information was never proven to have occurred, was that in so proving this claim will require a good deal of computer knowledge. We see in the Court's order and opinion that some defendants admitted that their apps were taking address book data without permission. Intervenor request that plaintiffs be allowed to prove that the data is being taken, for UCL claim purposes:

1) Plaintiffs allege that data is being sent without permission over Wifi connection
2) Plaintiffs should disable router encryption (Wep, WPA, etc) so that all packets will be plaintext when sent to router
3) Connect their idevices to their router wifi
4) On a secondary laptop, the plaintiffs need to install a wireless sniffer; such as Wireshark (laptop will need wireless adapter)
5) Once Wireshark is installed, plaintiffs should "sniff" (capture) packets sent wirelessly to their router (Note: a special driver may need to be installed also -Google-)
6) On their idevice, load up the app that is alleged to have stolen data, the laptop should detect any packets being sent
7) If all is done right, plaintiffs will see this information as packets and the server site these packets are being sent to

This will show property being lost/or taken, if done correctly. and once again, for Windows OS running Wireshark may require a special airpcap driver -plaintiffs should contact their cyber security consultants for this

Intervenor claims, as do these plaintiffs, that Apple misled the public about the integrity of its Iphone. Apple claims that apps could not access data from other apps, and, unfortunately, these apps can and do. Not only that, but according to the defendant's admissions, Websites are able to send and receive data too. When intervenor was able to get ahold of his Iphone in the summer of 2012, he as did plaintiffs, relied upon the statements concerning reputation of Iphones on Apple's website, Itunes, and IOS discussions and excerpts. These misrepresentations led him, and othe plaintiffs, into obtaining an Iphone, and had intervenor realized the extent of the lack of perceived security then, as opposed to when he developed his first Hello World tutorial and realized how easy it was for apps to access privat data, plaintiffs, and intervenor would have held off on purchasing; and waited until more secure models were available. Intervenor would like Apple Inc to send him a newer model Iphone as relief; maybe even for beta testing too.

Concerning the App store, we can find Apple's developers' representations, that all app store apps are reviewed and screened for privacy and safety reasons. This can be found on the Apple App store website, Itunes agreements, and developer sites to Apple. In order to state a claim under California law, the conduct MUST constitute, "unfair, deceptive, untrue or misleading advertising." (Cal. Bus. and Prof. Code §17500) and, a FAL claim is only sound if a reasonable person is deceived by the allegedly false advertising (Williams v. Gerber Products Co. 552 F.3d 934)

Apple and its idevices did not have the app notification screen that Android devices do. (Android will tell the user what the App will access on the device such as Contacts, text messaging etc) As a malware writer for educational purposes, your intervenor can clearly say for the record, that any archive or server that hosts malware for educational purposes does notify the user that these programs are capable of harm, or accessing sensitive information, and debugging or decoding may result in said harm to the system. Codes are free speech, but fair practice and process to the general public is a requirement on the internet these days.

Certificate of Service

I, Justin Credico, intervenor in this captioned case, do hereby verify that on this 13th day of November 2014, one true copy of this enclosed Motion to Intervene, has been sent via first class mail to the following:

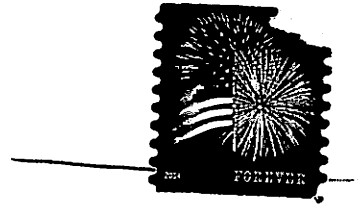
Clerk of Courts
United States District Court
for the Northern District of
California
1301 Clay Street
Oakland California 94612

11-13-14
Date

Justin Credico
pro se

Justin Credico
#71239-066
Federal Detention Center
700 Arch St
PO Box 562
Philadelphia PA 19105

legal mail



Clerk of Courts
United States District Court
Northern District of California
1301 Clay Street
Oakland California 94612

94612$5212